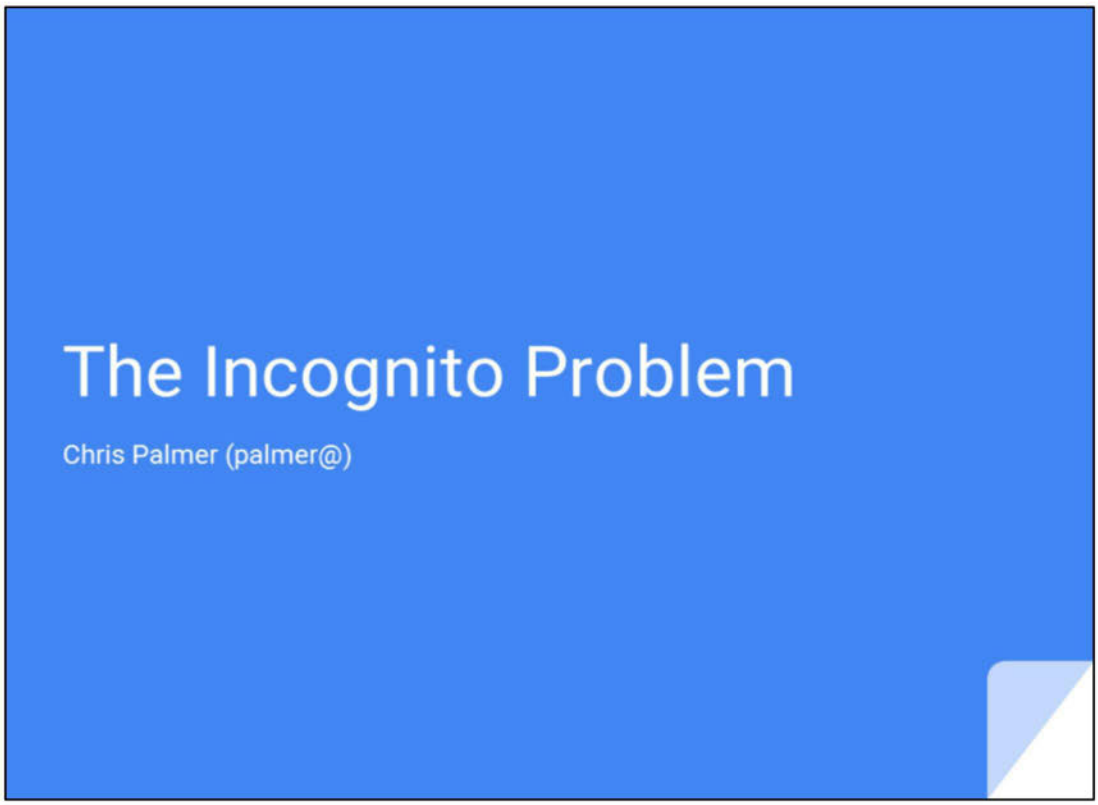
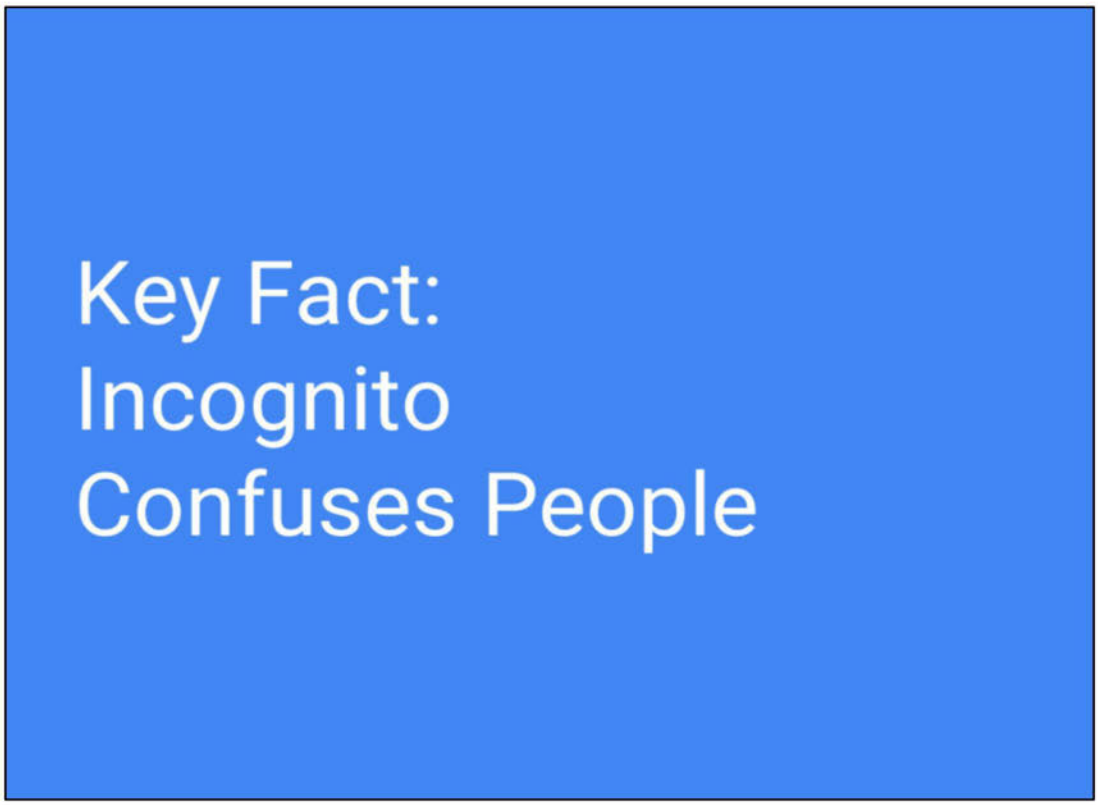
Exhibit 28

Omnibus Mao Declaration


The Incognito Problem
Chris Palmer (palmer@)


Key Fact:
Incognito
Confuses People

“Incognito” Confuses People

We know from intuition, anecdotes, and now empirically (Yuxi Wu, et al.; see also Habib, et al.) that the “incognito”/Spy Guy branding, and the complex disclosures (like all complex disclosures), confuse people as to what exact guarantees it offers and does not offer.

Ironically, across all browsers, Chrome’s disclosures were the least confusing by a modest amount. But it’s still bad.

Id	Date	Text
1	07/22/2018 07:53:36	It'd be good to try to replicate or further validate the study, but I'd be surprised if we got a significantly different result.

Table 5: Scenarios where participants held misconceptions, shown with the correct answers and percentage of participants who gave incorrect answers. For comparative scenarios, (in)equality symbols denote the correct answer, and we give the sum of all participants answering otherwise.

Scenario	Answer		% Incorrect	
	Std.	Priv.	Std.	Priv.
Overestimating private mode's privacy protections				
Search queries associated (logged in)	Yes	Yes	1.5	56.3
Bookmarks saved across sessions	Yes	Yes	25.4	46.5
Geolocation can be estimated	Yes	Yes	5.2	40.2
Employer can track browsing	Yes	Yes	1.1	37.0
Better protected from viruses/malware	Std. = Priv.		27.1	
IP address can be collected	Yes	Yes	0.7	25.2
Government can track browsing	Yes	Yes	4.1	22.6
ISP can track browsing	Yes	Yes	3.0	22.0
Underestimating private mode's privacy protections				
Downloaded file in browser's list	Yes	No*	1.3	51.7
Proportion of targeted ads	Std. > Priv.		30.9	
Search queries associated (not logged in)	Yes	No	20.2	30.0

*Except in Brave's private mode, which does retain download history

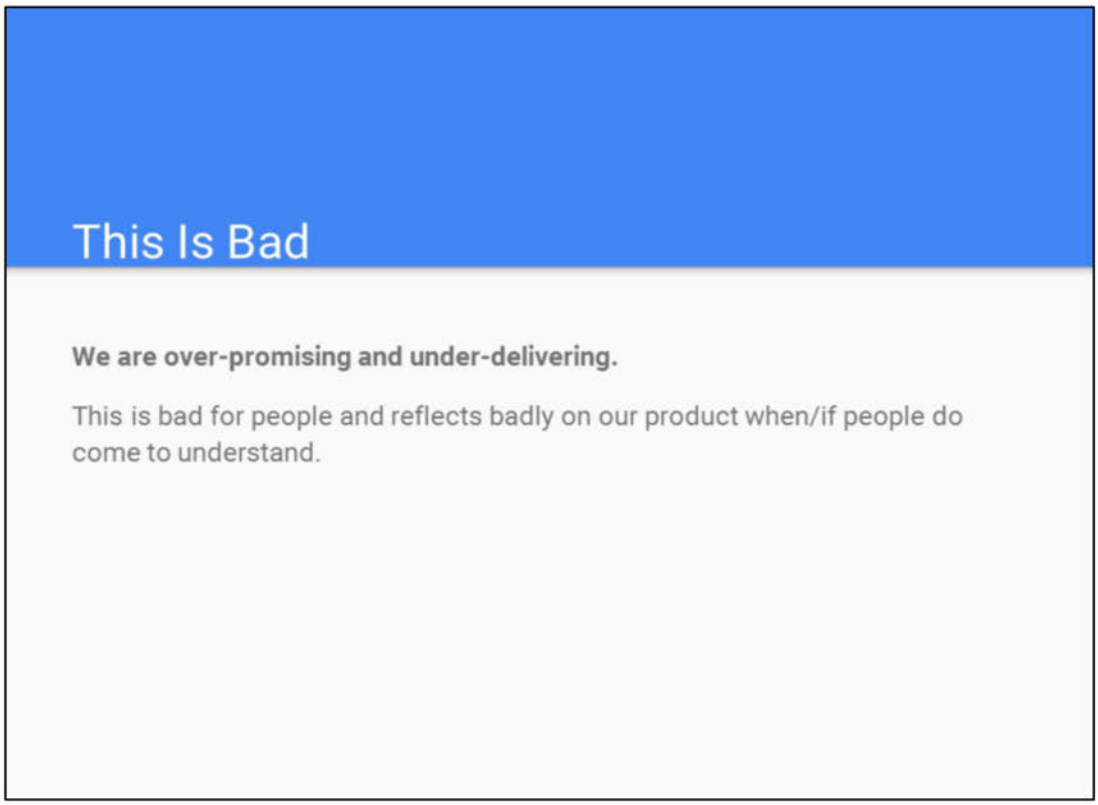
Table 6: Distinguishing scenarios where private mode's impact depends on the browser or context.

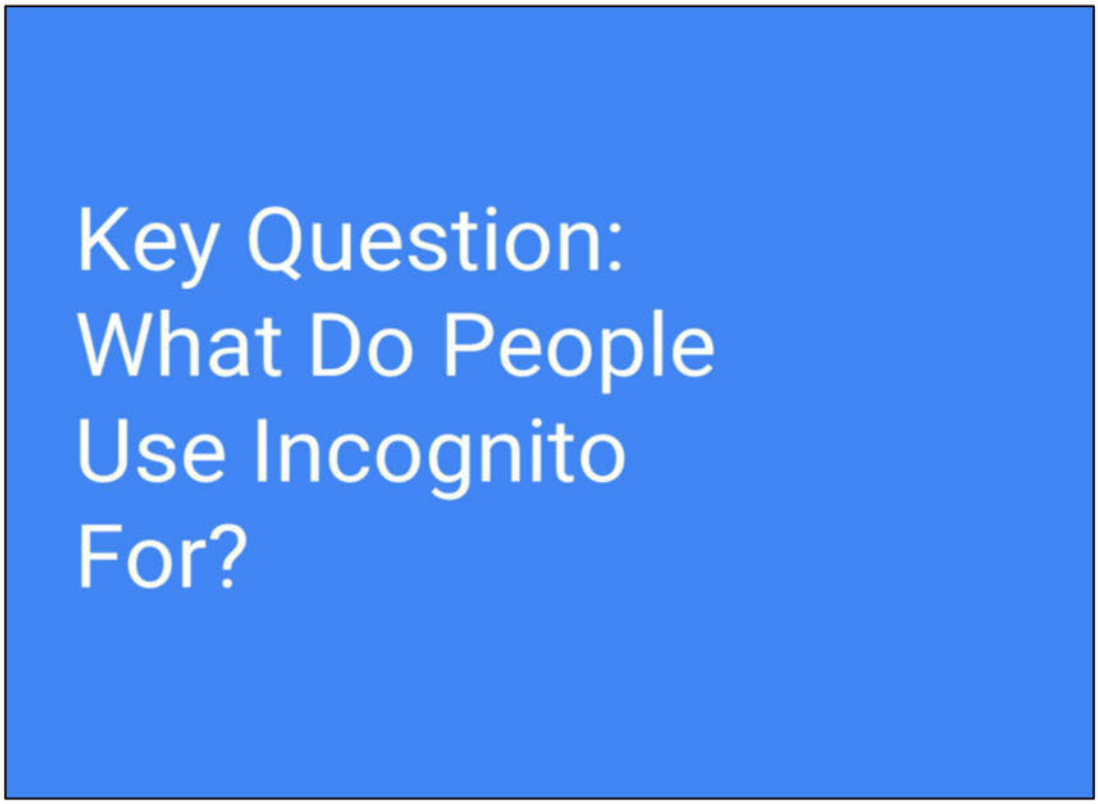
Scenario	% Yes	
	Std.	Priv.
Items in shopping cart saved across sessions	97.8	78.8
Browser extensions active across sessions	98.3	69.1
Forensic expert can reconstruct browsing history	98.7	52.8
Site-specific preferences (e.g., for pop-ups) saved	98.3	31.3

Table 7: Distribution of responses for comparative scenarios where the impact depends on the browser or context.

Scenario	% Responses		
	Std. > Priv.	Std. = Priv.	Std. < Priv.
Amount of ads	32.2	64.9	2.9
Page loading speed	24.8	53.6	21.6

($\chi^2(12) = 38.1, p = .001$). In the control condition, 32.4% of participants mistakenly believed downloaded files would still be listed in the browser. A higher proportion of participants in Brave (62.2%,


This Is Bad
We are over-promising and under-delivering.
This is bad for people and reflects badly on our product when/if people do come to understand.


Key Question:
What Do People
Use Incognito
For?

Why Do People Use Private Modes?

From Wu, et al.:

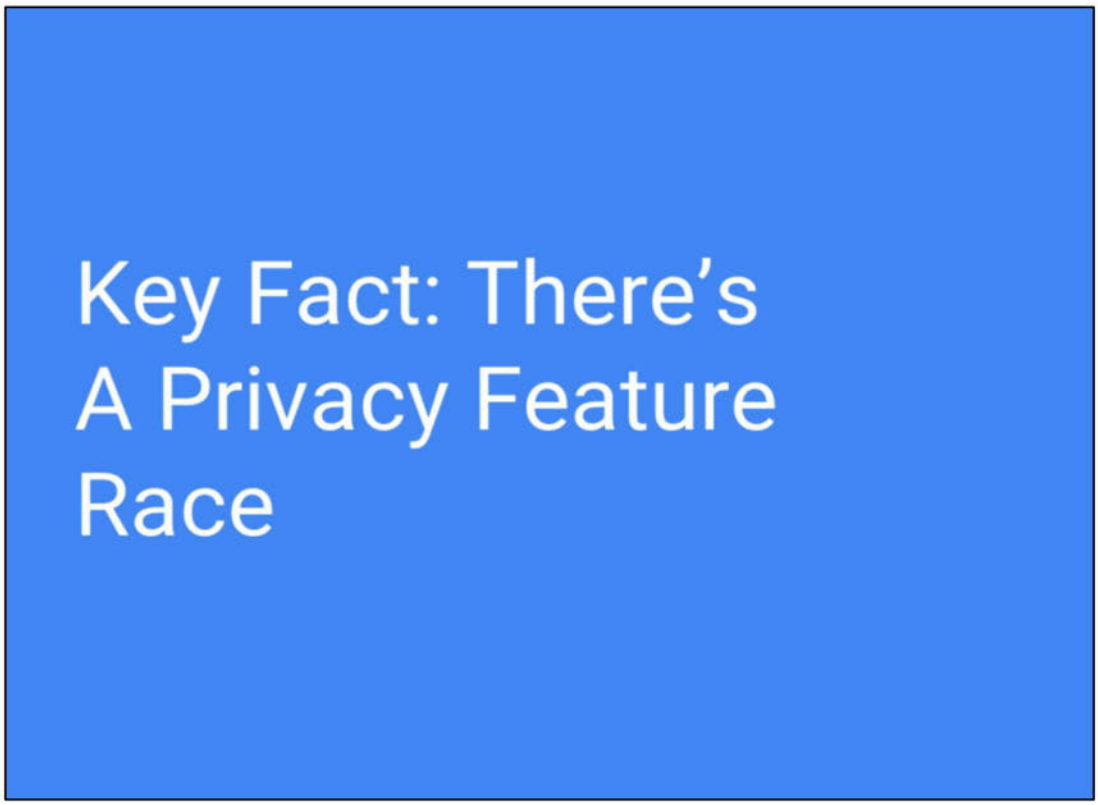
1. Hide browsing history, especially visits to adult websites;
2. prevent targeted ads and search suggestions;
3. achieve "safer" browsing;
4. Prevent browsers from saving login-related information;
5. avoid cookies;
6. accommodate intentional or unintentional use by others.

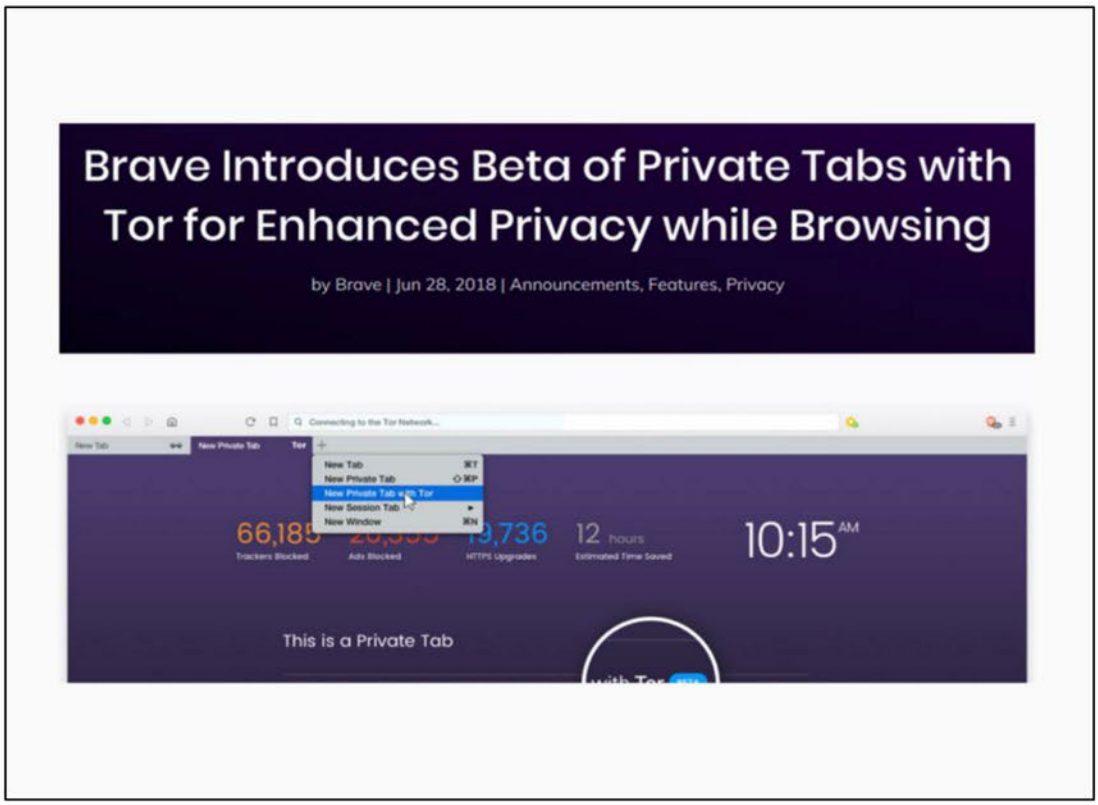
Id	Date	Text
1	07/23/2018 13:28:04	what's the motivation here? how does this differ from 2?
2	07/23/2018 13:28:04	This is a list of reasons that people reported to the researchers for why they use private browsing modes. Part of the point of the research is that people don't fully understand the mechanisms.

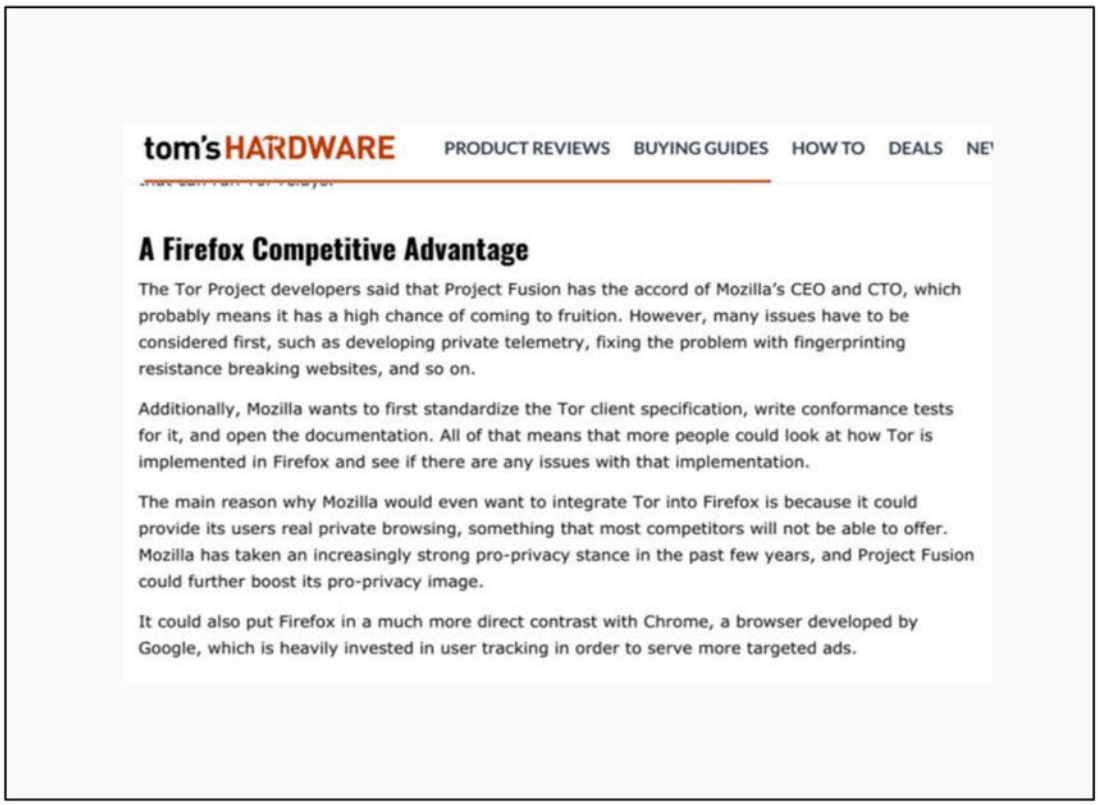
Incognito Is Overloaded

Those 6 reasons are related but different. Perhaps we really need multiple modes (we've already got Guest mode)?

Or more and easier affordances for privacy and control in Settings/elsewhere?


Key Fact: There's
A Privacy Feature
Race


Brave Introduces Beta of Private Tabs with Tor for Enhanced Privacy while Browsing
by Brave | Jun 28, 2018 | Announcements, Features, Privacy
New Tab
New Private Tab
New Private Tab with Tor
New Session Tab
New Window
66,185
Trackers Blocked
19,736
HTTPS Upgrades
12 hours
Estimated Time Saved
10:15 AM
This is a Private Tab



tom's HARDWARE PRODUCT REVIEWS BUYING GUIDES HOW TO DEALS NE

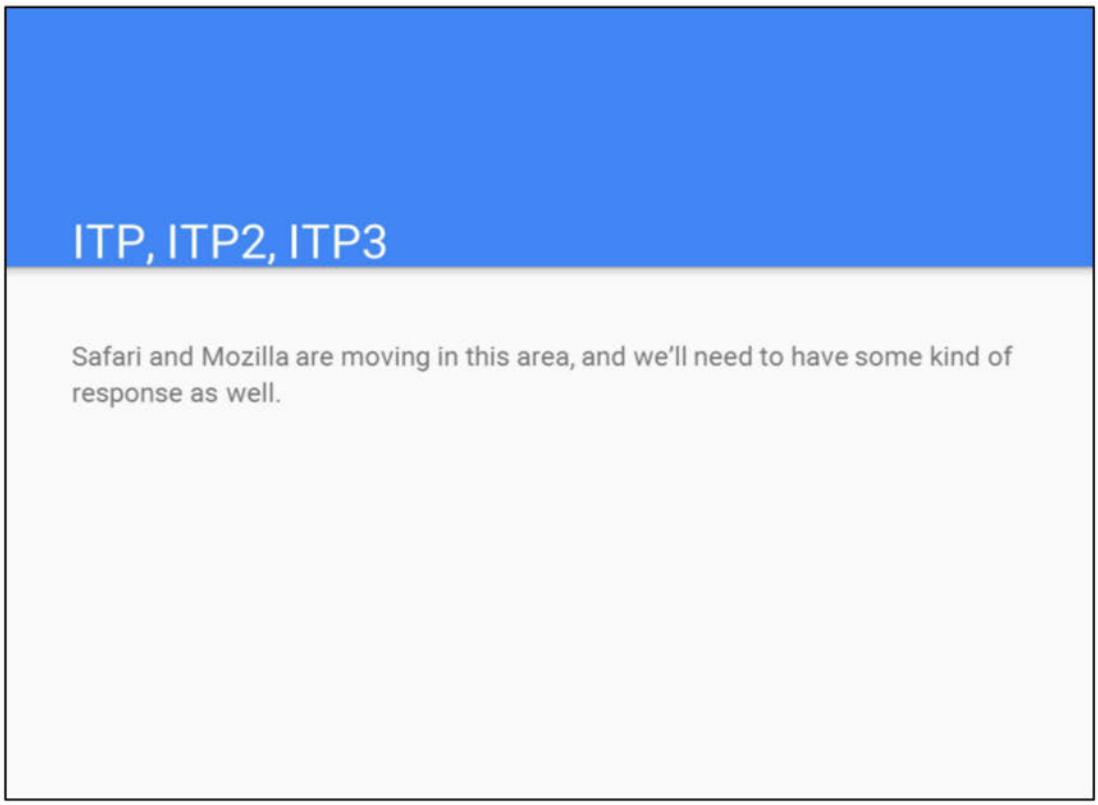
A Firefox Competitive Advantage

The Tor Project developers said that Project Fusion has the accord of Mozilla's CEO and CTO, which probably means it has a high chance of coming to fruition. However, many issues have to be considered first, such as developing private telemetry, fixing the problem with fingerprinting resistance breaking websites, and so on.

Additionally, Mozilla wants to first standardize the Tor client specification, write conformance tests for it, and open the documentation. All of that means that more people could look at how Tor is implemented in Firefox and see if there are any issues with that implementation.

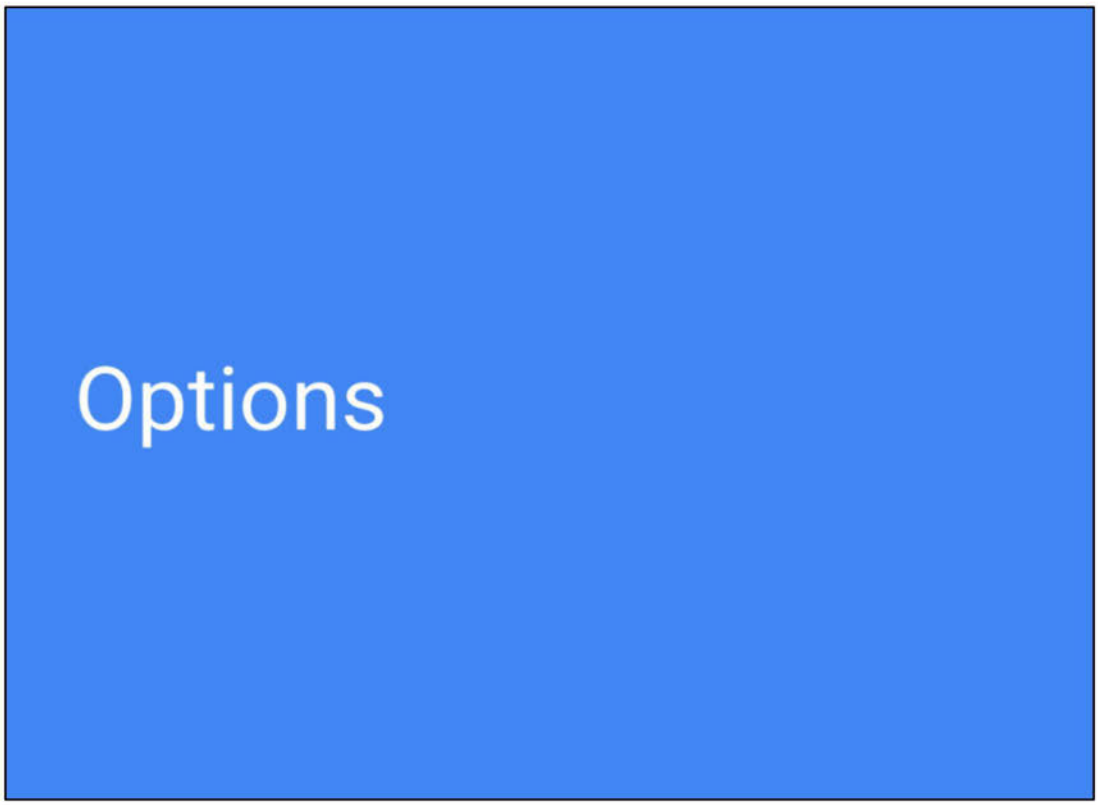
The main reason why Mozilla would even want to integrate Tor into Firefox is because it could provide its users real private browsing, something that most competitors will not be able to offer. Mozilla has taken an increasingly strong pro-privacy stance in the past few years, and Project Fusion could further boost its pro-privacy image.

It could also put Firefox in a much more direct contrast with Chrome, a browser developed by Google, which is heavily invested in user tracking in order to serve more targeted ads.


ITP, ITP2, ITP3
Safari and Mozilla are moving in this area, and we'll need to have some kind of response as well.


[redacted]

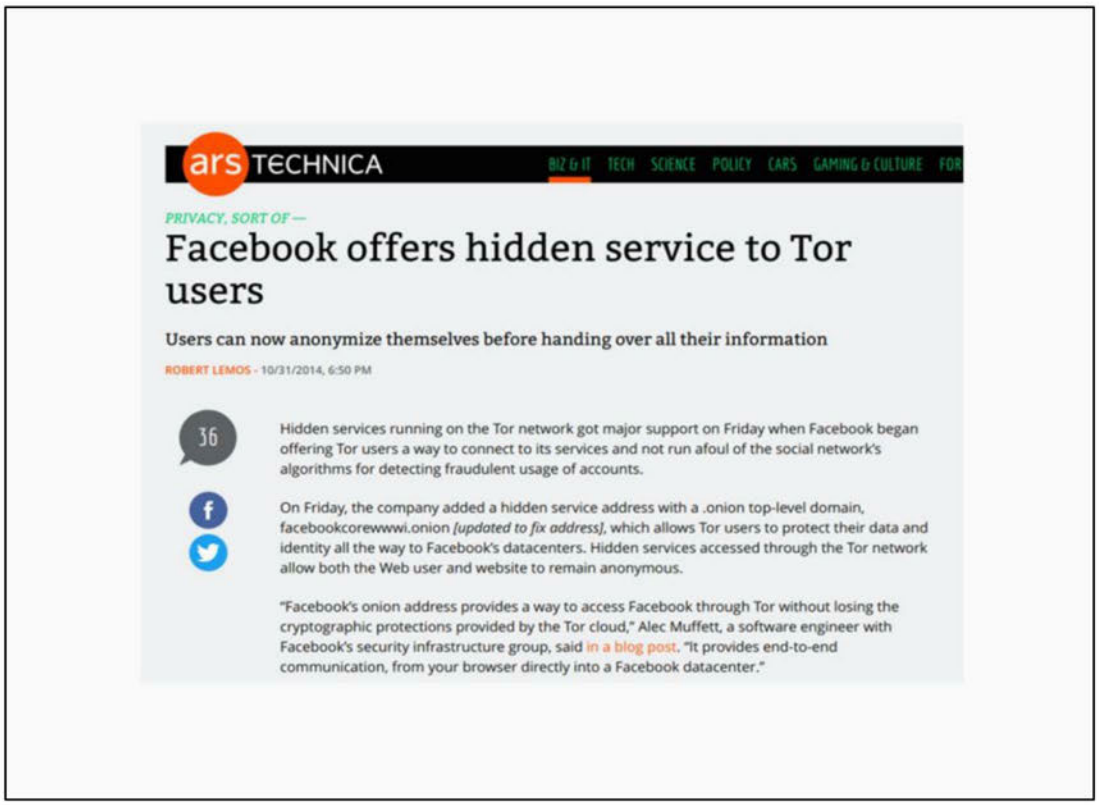
Id	Date	Text
1	07/21/2018 14:10:10	[redacted]


Options


[redacted]


[redacted]

Id	Date	Text
1	07/23/2018 14:04:19	[redacted]
1	07/23/2018 14:05:29	[redacted]
2	07/23/2018 14:05:29	[redacted]



ars TECHNICA BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE FOR

PRIVACY, SORT OF —

Facebook offers hidden service to Tor users

Users can now anonymize themselves before handing over all their information

ROBERT LEMOS - 10/31/2014, 6:50 PM

36

Hidden services running on the Tor network got major support on Friday when Facebook began offering Tor users a way to connect to its services and not run afoul of the social network's algorithms for detecting fraudulent usage of accounts.

On Friday, the company added a hidden service address with a .onion top-level domain, facebookcorewwwi.onion *[updated to fix address]*, which allows Tor users to protect their data and identity all the way to Facebook's datacenters. Hidden services accessed through the Tor network allow both the Web user and website to remain anonymous.

"Facebook's onion address provides a way to access Facebook through Tor without losing the cryptographic protections provided by the Tor cloud," Alec Muffett, a software engineer with Facebook's security infrastructure group, said in a blog post. "It provides end-to-end communication, from your browser directly into a Facebook datacenter."

MOBILE

Facebook's latest privacy debacle points to larger problem: Trust

The social network is in hot water over a VPN security app it owns called Onavo reportedly spying on users. But Facebook's issues are deeper than that.

BY RICHARD NIEVA / FEBRUARY 14, 2018 1:41 PM PST

Most VPN Services are Terrible

Short version: I strongly *do not* recommend using any of these providers. You are, of course, free to use whatever you like. My TL;DR advice: Roll your own and use Algo or Streisand. For messaging & voice, use Signal. For increased anonymity, use Tor for desktop (though recognize that doing so may actually put you at greater risk), and Onion Browser for mobile.

This mini-rant came on the heels of an interesting twitter discussion:
https://twitter.com/kennwhite/status/591074055018582016

Again I strongly do *not* recommend using any of these providers.

Provider / known "Secret" Key

```
Astril / way2stars
EarthVPN / earthvpn
GFWVPN / gfwvpn
GoldenFrog / thisisourkey
IBVPN / ibVPNsharedPSK!
IPVanish / ipvanish
NordVPN  / nordvpn
PrivateInternetAccess (PIA) / mysafety
PureVPN / 12345678
SlickVPN / gogoVPN
TorGuard / torguard
TigerVPN / tigerVPN
```

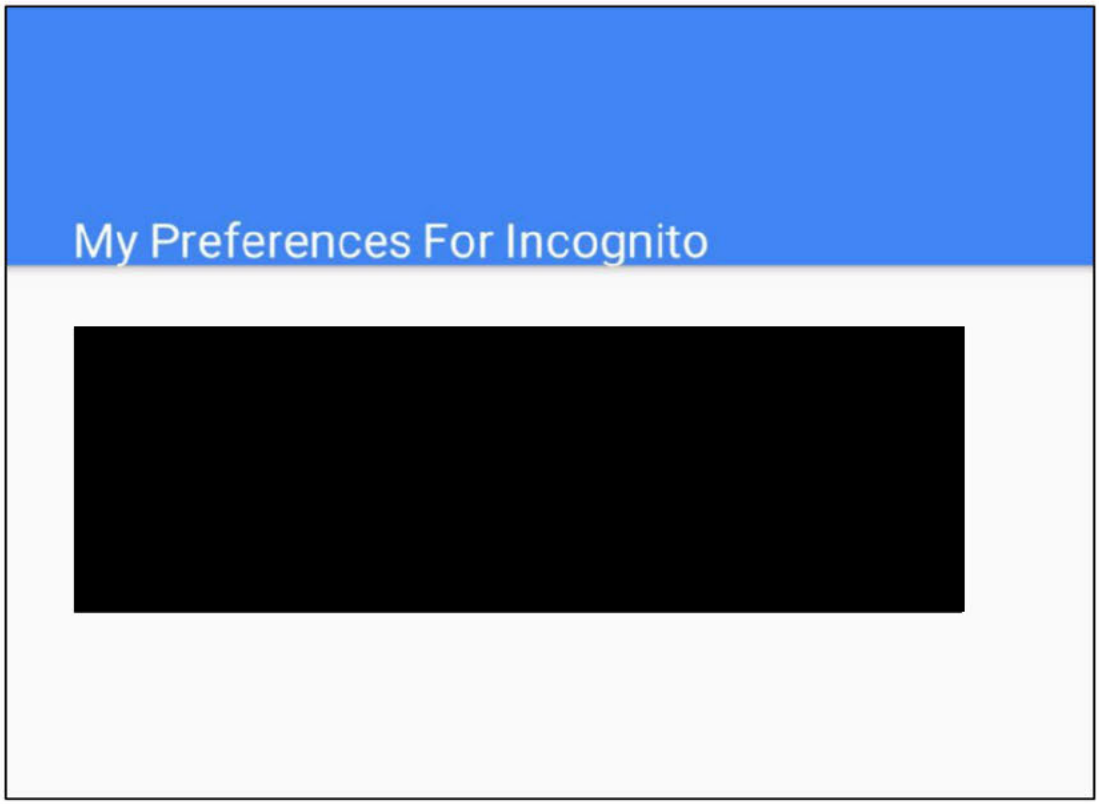
source: https://gist.github.com/kennwhite/1f3bc4d889b02b35d8aa


There Is Some Opportunity, Though

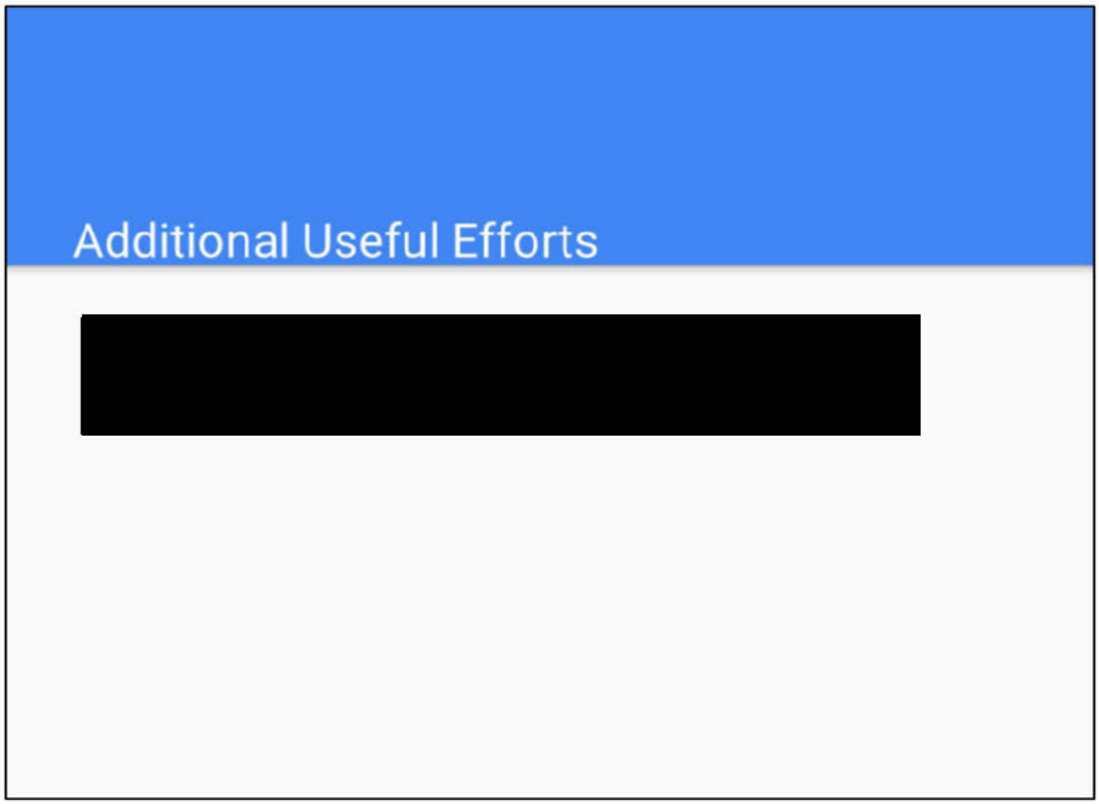
Key Question:
How Much
Breakage Will
People Tolerate?

Hypothesis: Not Much

Conclusion: Options, But No Single Clear Path


My Preferences For Incognito

Id	Date	Text
1	07/21/2018 15:50:53	[redacted]
3	07/22/2018 08:00:43	[redacted]
2	07/23/2018 12:54:42	[redacted]
3	07/23/2018 12:54:42	[redacted]


Additional Useful Efforts
[redacted]

PRODBEG: GOOG-BRWN-00140297
PRODBEGATT:
PRODEND: GOOG-BRWN-00140329
PRODENDATT:
PRODVOL: PROD023
2nd_CROSS_BEGBATES:
2nd_CROSS_ENDBATES:
AllCustodians: AbdelKarim Mardini;Alexei Svitkine;Helen Harris
TO:
FROM:
CC:
BCC:
CONFIDENTIALITY: Confidential
CROSS_ALLCUSTODIANS: AbdelKarim Mardini;Alexei Svitkine;Helen Harris
CROSS_ATTACHMENTNAME:
CROSS_BEGATTACH:
CROSS_BEGBATES: GOOG-CABR-00094818
CROSS_CC:
CROSS_CONFIDENTIALITY: CONFIDENTIAL
CROSS_CUSTODIAN: Alexei Svitkine
CROSS_DATECREATED: 07/21/2018
CROSS_DATEMOD: 10/09/2019
CROSS_DATERECEIVED:
CROSS_DATESENT:
CROSS_DE-DUPED CUSTODIANS: AbdelKarim Mardini;Alexei Svitkine;Helen Harris
CROSS_ENDATTACH:
CROSS_ENDBATES: GOOG-CABR-00094850
CROSS_FILEEXTENSION: pptx
CROSS_FILENAME: The Incognito Problem_1TNOMivlbk0cAiQqY4twyccyjRYGHydry4vVWjt1h0-t4.pptx
CROSS_FROM:
CROSS_MD5 HASH: D073B8D9E8F4A04FB597F6D6AD115E38
CROSS_MESSAGE ID:
CROSS_OWNER: palmer@google.com
CROSS_PRODVAL: CROSS-PROD002
CROSS_REDACTED: N
CROSS_SUBJECT:
CROSS_TITLE: The Incognito Problem
CROSS_TO:
CUSTODIAN/SOURCE: Alexei Svitkine
DATECREATED: 07/21/2018
DATELASTMOD: 10/09/2019
DATERCVD:
DATESENT:
DeDupedCustodians:
DOCEXT:
FILENAME: The Incognito Problem_1TNOMivlbk0cAiQqY4twyccyjRYGHydry4vVWjt1h0t4.pptx
ILS_ProdDate: 06/18/2021
CROSS_ILS_ProdDate: 09/01/2021
MD5 HASH: D073B8D9E8F4A04FB597F6D6AD115E38
MessageID:
NATIVEFILE:
Owner: palmer@google.com
PAGES:

REDACTED: N
SUBJECT: